NIH Wireless Network Security Standards

October 8, 2002 (VERSION 20021008.1)

Due to the security vulnerabilities that exist in the wireless networking protocols and devices, it is necessary that security be the main focus before deploying wireless networking devices at the NIH. In conjunction with the NIH Wireless Network Policy, this document addresses the minimum requirements and lists some recommendations for secure wireless network device deployment on and off NIH campus.

Requirements

- Register all Access Points (APs) as outlined in the NIH Wireless Network Policy.
- Once authenticated to an access point, users must either be routed outside the NIH firewall(s), or authenticate to an NIH network. Just as with a wired network, NIH network authentication, whether NIH-wide or IC-specific, must satisfy prescribed login/password combinations prior to using NIH or IC-specific resources that are not normally accessible by nodes outside the NIH firewall(s).
- Ensure the wireless device satisfies any existing Radio Frequency Interference (RFI) standards.
- Assign APs static IP addresses. APs cannot be deployed in a dynamic IP environment.
- Change all default ESSID/SSIDs from their default vendor settings to unique names.
- If SNMP is turned on for management purposes, change SNMP Community strings from their manufacturer default to unique and difficult to guess strings.
- Install APs in a properly secured, adequately monitored area to prevent unauthorized access and physical tampering. Devices should not be placed in easily accessible public locations.
- Employ an encryption protocol between any two wireless devices. WEP (or equivalent) must be implemented with some form of encryption (40 bit, 64 bit, and 128 bit).
- All APs and clients must be in compliance with the NIH Password Policy at http://irm.cit.nih.gov/policy/passwords.html, and the NIH Warning Banner Policy at http://irm.cit.nih.gov/policy/warnbanners.html.
- Segregate Wireless LANs from traditional wired LANs through the use of firewalls, separate VLANs and/or DMZs.
- Unless appropriate security is employed (e.g. 128-bit or higher encryption, multiple levels of authentication and security), avoid the use of Wireless LANs for the transmission of sensitive data (e.g. patient data, financial data).

Recommendations

The following are recommendations to further enhance the security of a wireless network. Where feasible, consider adopting these recommendations in addition to the requirements listed above.

- Employ WEP (or equivalent) at 128 bit or better encryption. However, do not rely on WEP alone as a security solution.
- For APs that use public IP space, register DNS entries using NIH naming conventions.
- Employ MAC-based authentication by only allowing registered MAC addresses access to the AP.
- Employ multiple levels of authentication and security. Recommendations include the use of RADIUS, PKI and Virtual Private Network (VPN) services. If single logon and password are required, the use of the NIH Active Directory Database is also recommended.
- Due to the nature of wireless sniffing devices, changing the SSID string from the default and removing SSID broadcasting are options that offer limited security. To further enhance security of APs, employ a non-trivial and difficult to guess ESSID/SSID of 10 or more characters in length.
- Avoid broadcasting to areas not intended for service. Locate APs centrally within the intended area of service and avoid placing APs near windows or against the outside walls of buildings.

Glossary

NIH Firewall – The NIH firewall is a network device used to block unauthorized network traffic from entering NIHnet.

NIHnet – NIHnet is the name used to designate the NIH backbone computer network and all subnetworks attached to the NIH backbone.

Sensitive Data – Sensitive data are data that require protection due to the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration, or destruction of the data. The term includes data whose improper use or disclosure could adversely affect the ability of an agency to accomplish its mission, proprietary data, records about individuals requiring protection under the Privacy Act, and data not releasable under the Freedom of Information Act.

Service Set Identifiers (SSID) – A unique indentifier attached to the header of packets sent over a LAWN (Local Area Wireless Network). It is primarily intended to differentiate LAWNs, but also acts as a rudimentary password.

Wireless – A technology that permits the transfer of information (active or passive) between separate points using electromagnetic waves rather than a physical connection.